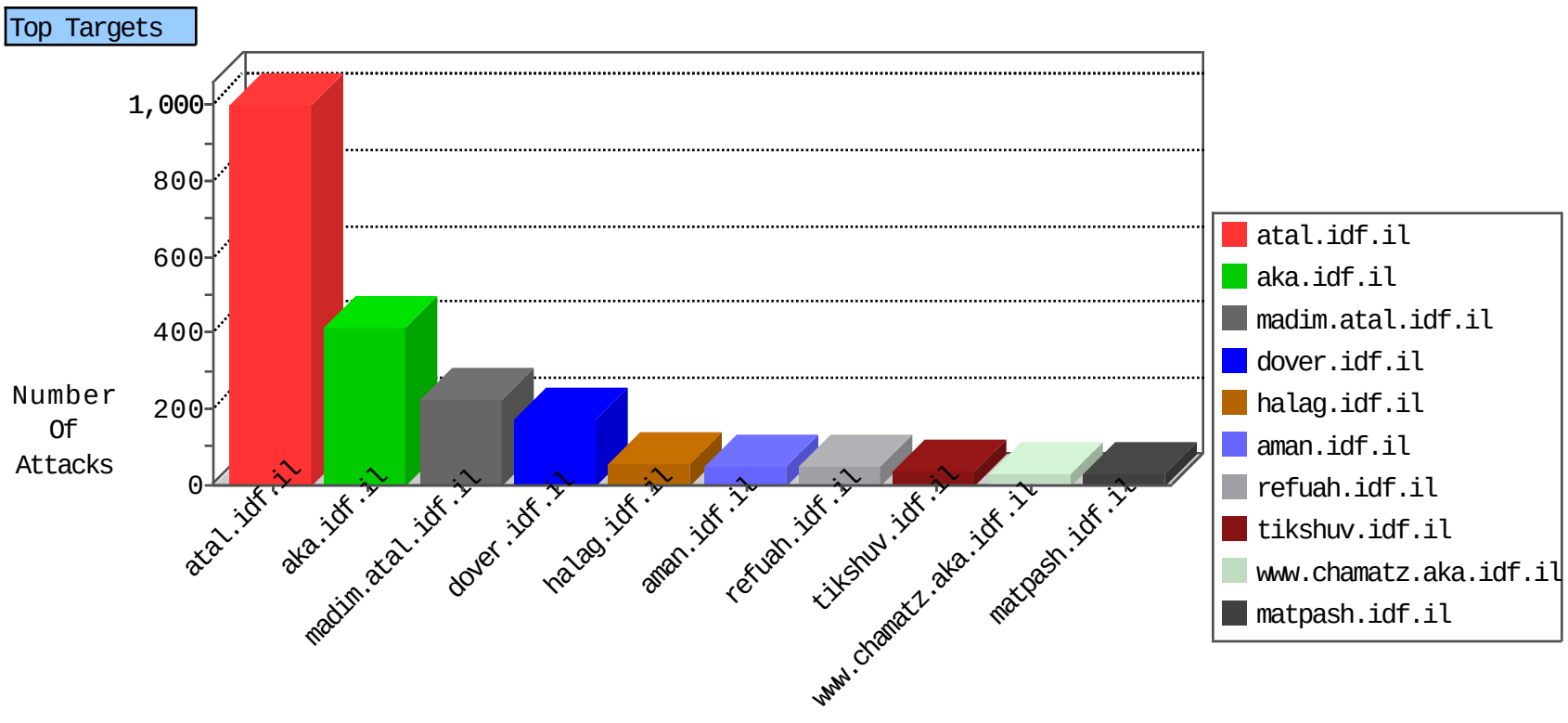
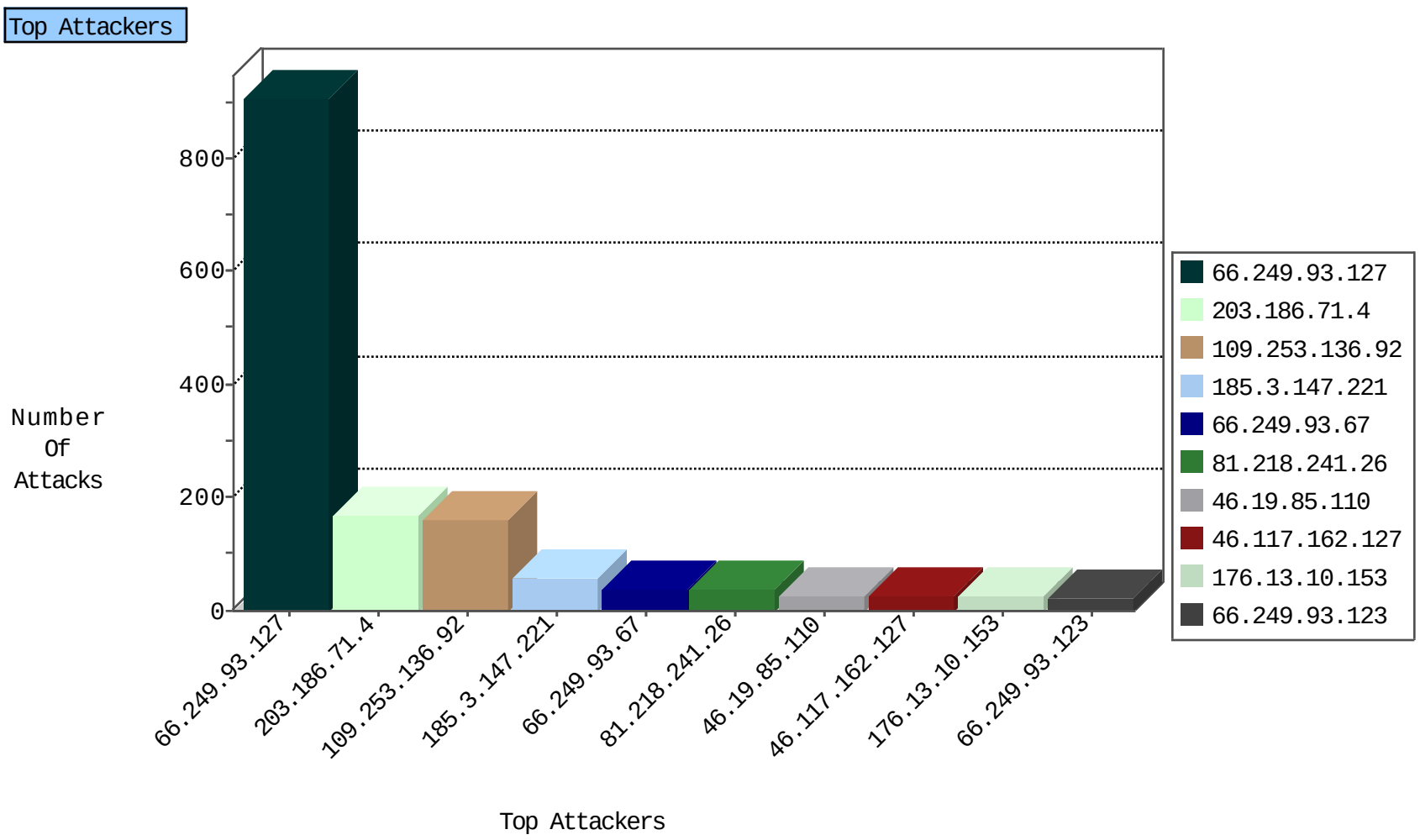
03-08-2016-16:04:09 to 03-08-2016-17:04:09

IDF Under Attack Daily Report



Top Target



Top Attackers

03-08-2016-16:04:09 to 03-08-2016-17:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

03-08-2016-16:04:09 to 03-08-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
217.132.108.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.20.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.37.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.247	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.147.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.75	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.95.218	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.87	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.68	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.95.76	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.90	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.239	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.95.102	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.95.168	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-08-2016-16:04:09 to 03-08-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	877
81.218.118.126	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
5.102.254.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.114.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
213.8.204.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.76.86	Hong Kong	navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.146.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.209.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.82.220	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.37.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
137.226.113.7	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
46.19.85.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.22.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.217.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
79.179.172.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.37.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
61.244.49.137	147.237.8.24	Hong Kong	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
178.162.211.200	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.199.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.226.113.7	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
46.19.85.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.205.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.45.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.140.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-08-2016-16:04:09 to 03-08-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.147.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	38
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
176.13.10.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
203.186.71.4	Hong Kong	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	24
46.117.162.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
2.52.131.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.124	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
195.145.36.16	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.111.70.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.71.0.177	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
182.68.165.74	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.139.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.30.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
182.68.165.74	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.84.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
203.186.71.4	Hong Kong	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
62.219.236.219	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.143.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.84.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.64.193	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
103.21.58.191	India	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
147.236.238.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
147.236.238.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.5.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
89.138.207.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.128.143	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.130.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.200.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.204.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.195.16	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.184.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
46.117.204.235	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.230.86.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-08-2016-16:04:09 to 03-08-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.136.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
203.186.71.4	Hong Kong	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 203.186.71.4	Block	71
203.186.71.4	Hong Kong	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	24
176.13.18.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
203.186.71.4	Hong Kong	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	7
203.186.71.4	Hong Kong	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	7
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
62.128.41.133	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	4
2.54.178.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
203.186.71.4	Hong Kong	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	4
203.186.71.4	Hong Kong	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	4
203.186.71.4	Hong Kong	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	4
203.186.71.4	Hong Kong	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 203.186.71.4	Block	4
109.253.204.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.76.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.195.239	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.108.71.93	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.8.30.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
2.54.13.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
203.186.71.4	Hong Kong	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.146.182	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
183.206.160.57	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.206.160.57	Block	2
66.249.93.98	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/favicon.ico	Block	1
203.186.71.4	Hong Kong	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
141.212.122.209	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.65.72.216	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
203.186.71.4	Hong Kong	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
185.3.147.221	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
89.139.234.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.1.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
212.179.243.124	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
203.186.71.4	Hong Kong	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized Method for Known URL from 203.186.71.4	None	1
94.230.93.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.160.57	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/scripts/fckeditor/editor/	Block	1
149.78.60.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.93.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
203.186.71.4	Hong Kong	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
109.65.199.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.220.155.215	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
185.88.24.168		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
93.173.52.147	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 93.173.52.147 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
178.54.21.27	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
80.246.140.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.143.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-08-2016-16:04:09 to 03-08-2016-17:04:09